

REMARKS

By this Amendment, Applicant amends claims 1, 5, 12, 13, 16, 17, 21, 28, and 29. Claims 1-6, 12, 13, 16-22, and 28-30 are currently pending.

In the Office Action, the Examiner rejected claims 1-6, 12, 13, 16-22, and 28-30 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Application Publication No. 2002/0029200A1 to Dulin et al. (hereinafter "Dulin") in view of U.S. Patent Application Publication No. 2002/0166049 to Sinn (hereinafter "Sinn").

Regarding the Response to Arguments

The Examiner alleged that newly cited reference Dulin "teaches the step of "sending by the OCSP responder, the database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid" at page 6, [0081]." (Office Action at 15.) Applicant respectfully disagrees.

At page 6, [0081], Dulin teaches that "issuing participant 102 checks its customer database 214_{IP} to make sure that the request was signed by an entity authorized to make the request." (emphasis added.) That is, "issuing participant 102 verifies transaction coordinator 202_{RP}'s signature on the request using the relying participant's transaction coordinator certificate (sent with the request) and the root public key (which may be stored in hardware security module 218_{IP})." Dulin, page 6, [0082]. Therefore, Dulin's teaching of checking customer database 214_{IP} for signature on the request does not constitute a teaching of "sending by the OCSP responder, the database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid," as recited by claim 1 (emphasis added).

Regarding the Rejections Under 35 U.S.C. § 103

Applicant respectfully traverses the Examiner's rejection of claims 1-6, 12, 13, 16-22, and 28-30 under 35 U.S.C. § 103. In order to establish a prima facie case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim elements. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Third, there must be a reasonable expectation of success. See M.P.E.P. § 2143.

As explained above, Dulin fails to teach or suggest at least "sending by the OCSP responder, the database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid," as recited by independent claim 1. Further, in order to expedite the prosecution of this application, claim 1 has been amended to recite a combination including, for example, "receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked_expired."" Dulin fails to teach or suggest at least "receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate

information reflecting status of the certificate, permissible values of the certificate information including at least “valid,” “invalid,” “revoked,” “expired,” and “revoked_expired,”” as recited by amended claim 1.

Dulin teaches a “four-corner model comprises a first institution 102 and a second institution 104. First institution 102 is referred to as the “issuing participant” because it is a participant in the present system and issues smart cards to its customers.” Dulin, para [0032] at 2. “Second institution 104 is referred to as the “relying participant” because it is a participant in the present system and its customers rely on representations made by issuing participant 102 and issuing participant 102’s customers.” “Participants 102, 104 are typically banks or other financial institutions.” Dulin, para [0032] at 2. In Dulin, “each participant that receives an OCSP request for a certificate issued by another participant, forward the request to the issuing participant for that certificate.” “If the subscribing customer is a customer of a different participant, relying participant 104 generates a signed validation request for the subscribing customer’s certificate and sends it to the identified issuing participant 102 along with its own certificate.” Dulin, para [0079] at 5. To check the validity of the request, “issuing participant 102 checks its customer database 214_P to make sure that the request was signed by an entity authorized to make the request.” Dulin, para [0081] at 6.

However, Dulin’s teaching of verifying the request validity does not constitute a teaching of “receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate,

permissible values of the certificate information including at least “valid,” “invalid,” “revoked,” “expired,” and “revoked expired,”” as recited by amended claim 1.

Sinn fails to cure Dulin’s deficiencies. Sinn teaches a system for obtaining and maintaining certificate status. Sinn teaches that “Directory Server 36 is an LDAP Directory Server and communicates with other servers/modules using LDAP over SSL.” Sinn, para [0119] at 6. Sinn also teaches keeping certificate status information in Directory Server 36 which is neither associated with a certificate authority nor real time. “If a real time status check is required, Identity System 40 retrieves the requested certificate’s real time status from Certificate Authority 2084,” and “[i]f real time status checking was not request (step 3424), Identity Server 40 retrieves previously obtained real time status that is sgored in the Identity System for the certificate (step 3458).” Sinn, FIGs. 52, 59B, paras. [0397], [0401]. However, Sinn’s teaching of using an LDAP Directory Server keeping offline certificate status information does not constitute a teaching of “receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least “valid,” “invalid,” “revoked,” “expired,” and “revoked expired,”” as recited by amended claim 1 (emphasis added).

Moreover, Dulin and Sinn fail to provide any suggestion or motivation to combine reference teachings. The Examiner alleged that “it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Dulin and

Sinn's teachings to implement the certificate database using the well-know LDAP directory server as suggested by Sinn, in order to take advantage of the legacy LDAP directory server to store digital certificates instead of building a new database server for storing digital certificates, and therefore reduces the cost and the complexity of the system." Applicant respectfully disagrees. Dulin teaches issuing smart cards directly to customers and a "customer database" to "make sure that the request was signed by an entity authorized to make the request." Therefore, Dulin's teaching of the customer database cannot be combined with Sinn's teaching of an off-line certificate status database.

Therefore, neither Dulin nor Sinn, taken alone or in any reasonable combination, teaches or suggests all elements of claim 1. A prima facie case of obviousness cannot be established. Accordingly, Applicant respectfully requests withdrawal of the rejection of claim 1. Because claim 2 depends from claim 1, Applicant also requests withdrawal of the rejection of claim 2 for at least the same reasons stated above.

Independent claims 5, 12, 13, 16, 17, 21, 28, and 29, while of different scope, recite similar language as that of claim 1. Claims 5, 12, 13, 16, 17, 21, 28, and 29 are therefore also allowable for at least the same reasons stated above. Applicant respectfully requests withdrawal of the rejection of claims 5, 12, 13, 16, 17, 21, 28, and 29. Because claim 18 depends from claim 17, and claim 30 depends from claim 29, Applicant also requests withdrawal of the rejection of claims 18 and 30 for at least the same reasons stated above.

The Examiner alleged that "Dulin and Sinn teach the method, computer readable medium and system of claim 1, 17 as discussed above. Sinn further teaches a

Certificate Registration module (Fig. 54) for adding new digital certificates to the database.” (Office Action at 5.) Applicant respectfully disagrees.

As explained above, Dulin and Sinn fail to teach or suggest “receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least “valid,” “invalid,” “revoked,” “expired,” and “revoked_expired,”” as recited in claims 1 and 17. Further, Sinn fails to teach “sending an indication of a new digital certificate from the certificate authority to the certificate database upon issuance of the new digital certificate,” as recited by claims 3 and 19.

Sinn teaches that “[c]ertification registration module 2072 also retrieves approval responses, indicating whether issuing a certificate to the requesting user is allowed (step 2124).” “If enrollment is approved (step 2126), certificate registration module 2072 obtains a certificate for the user (step 2128).” Sinn, para. [0372] at 31. However, Sinn’s teaching of simply requesting a certificate from a certificate authority does not constitute “sending an indication of a new digital certificate from the certificate authority to the certificate database upon issuance of the new digital certificate,” as recited by claims 3 and 19 (emphasis added). Thus, Dulin and Sinn fail to teach or suggest all elements of claims 3 and 19. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 3 and 19 under 35 U.S.C. § 103 as being obvious from Dulin in view of Sinn.

Claims 4, 6, 20, and 22, while of different scope, recite similar language as that of claims 3 and 19. Claims 4, 6, 20, and 22 are therefore also allowable for at least the

same reasons stated above regarding the rejection of claims 3 and 19. Applicant respectfully requests withdrawal of the rejection of claims 4, 6, 20, and 22.

Conclusion


In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: April 5, 2005

By: 
Wenye Tan
Reg. No. 55,662